Multilateral Counter-Insurgency Networks

JOHN P. SULLIVAN and ROBERT J. BUNKER

Postmodern terrorism presents a significant challenge to global security and law enforcement institutions. Non-state actors operating across international borders, engaged in an apparent global insurgency of extremism that transects the traditional boundaries of crime and war, pose significant challenges to both intelligence and law enforcement agencies. These networked global insurgents blend political and religious fanaticism with criminal enterprises to challenge the rule of law and pose an epochal shift in the structures and relations among states. Negotiating this epochal shift requires traditional organs of national security (the diplomatic, military and intelligence services) to forge new partnerships with police and public safety organizations at the state and local (sub-national), as well as transnational levels. Significant operational, policy and cultural challenges must be overcome to forge an effective multi-lateral global network to counter global terrorism and insurgency.

Terrorism is a pervasive form of social and political violence that challenges state institutions and global security. As the 11 September 2001 (‘9/11’) attacks in New York and Washington, DC and the M-11 (*Eme Once*) attacks against the Madrid Metro illustrate, contemporary terrorism presents a significant challenge to global security and law enforcement institutions. Non-state actors operating across international borders, engaged in an apparent global insurgency of extremism that transects the traditional boundaries between national security and criminal enforcement, pose significant challenges to both intelligence and law enforcement agencies. Within a framework of global jihad that seeks an alternative to liberal global market-states, networked global insurgents are blending political and religious fanaticism with criminal enterprises to challenge the rule of law and exploit the seams between crime and war.

Existing security structures (domestically the police, and internationally the military and foreign intelligence services) designed to counter state-on-state threats find this new operational environment challenging at best. Preserving global and national security requires traditional organs of national

Low Intensity Conflict & Law Enforcement, Vol.11, No.2/3 (Winter 2002), pp.353–368
ISSN 0966-2847 print/ISSN 1744-0556 online
DOI: 10.1080/0966284042000279081 © 2004 Taylor & Francis Ltd

security (the diplomatic, military and intelligence services) to forge new partnerships with police and public safety organizations at the state and local (sub-national) level to effectively counter these threats. Significant operational, policy and cultural challenges must be overcome to forge an effective global network of public safety, law enforcement and traditional intelligence organizations to understand and anticipate current and evolving terrorist threats.

Terrorism and fourth generation warfare (4GW)[1] are significant elements of the contemporary (postmodern) threat environment. Links between religious extremists, criminal organizations (such as narcotics traffickers) and rogue state partners complicate civil and military responses to conflict. These new adversaries, a complex opposing force (OPFOR), are diverse and linked in unfamiliar ways.[2] They include a range of actors such as Osama bin Laden's Al Qaeda and its constellation of *jihadi* networks, as well as the loose coalition of criminal actors, guerrillas and insurgents that challenge and can be expected to continue to challenge national security capabilities that were designed to operate within a nation-state framework. Outside that framework, our traditional structures have great difficulties.[3]

In this threat environment, disruption and emerging threats can be expected to be as important as – or more important than – WMD issues. Effective response to these threats demands a high degree of interoperability among all levels of responders – local, state, federal – between a variety of disciplines (law enforcement, fire service, public health and medical), and between civil and military agencies. Intelligence is an important element of forging an interagency response. To be effective, this intelligence must embrace network attributes and effectively fuse with networked operational forces.

ORGANIZATIONAL AND FUNCTIONAL BASIS OF NETWORKS

Quite a bit of information exists on social network analysis and to a lesser degree the extension and/or modification of that analysis into the realm of conflict and war. Of direct interest is the organization of networks, network roles, network reaction cycle functioning, and potentials for better efficiency based on different levels of network analysis. This research is still in its infancy and fragmentary but synergies already exist which are aiding in the creation of counter-insurgency networks.

Network (Component) Organization

John Arquilla and David Ronfeldt's typology provides a basic overview of network organization and summarizes how individual nodes link to each other:[4]

> *Chain*: the chain or line network, as in a smuggling chain where people or goods, or information move along a line of separated contacts, and where end-to-end communication must travel through the intermediate nodes.
> *Star*: the hub, star, or wheel network, as in a franchise or a cartel where a set of actors are tied to a central (but not hierarchical) node or actor, and must go through that node to communicate and coordinate with each other.
> *All-channel*: the all-channel or full-matrix network, as in a collaborative network of militant peace groups where everybody is connected to everybody else.
> *Hybrid*: there may also be hybrids of the three types, with different tasks being organized around different types of networks.

To this typology can be added Phil William's perspective on nodal 'network roles', developed for criminal network analysis, but applicable for counter-insurgency networks if slightly modified:[5]

> *Organizers*: those core individuals and groups that provide the steering mechanism for the network.
> *Insulators*: individuals or groups whose role is essentially to insulate the core from the danger posed by infiltration and compromise.
> *Communicators*: individuals who ensure that communication flows effectively from one node to another across the network as a whole.
> *Guardians*: Enforcers concerned with the security of the network who take measures to minimize vulnerability to external attack or infiltration.
> *Extenders*: those whose role is to extend the network by recruiting new members and by negotiating with other networks regarding collaboration.
> *Monitors*: those who ensure the effectiveness of the network and whose responsibilities include reporting weaknesses and problems to the core organizers, who can then initiate remedial action.

Linking network structures to network roles offers better insights into how networks form. In the public domain simulated modeling of notional terrorist networks has taken place[6] as has modeling concerning the 19 Al Qaeda hijackers involved in the 9/11 attack.[7] This form of analysis is typically used to identify organizers which function as command and control nodes (C^2) and to show levels of contact and trust within the network. Modeling has also been used against criminal organizations, drug cartels and militant anarchist groups by law enforcement agencies using link analysis and other tools. Not enough of this modeling, however, is taking place to better understand and improve the capability of counter-insurgency networks.[8] Much of this problem stems from lack of resources for in house studies and the information itself, which is unavailable to independent researchers because of its sensitivity.

Network (Component) Function

A network, or the components of a network, will have various functions for conflict and war. Based upon the OODA (observe-orient-decide-act) loop model[9] a basic breakdown of these functions would be as follows:

Observe: sensors, scouts, intelligence (gathering)
Orient: intelligence (analysis)
Decide: headquarters staff (military)/officer-in-charge (police)
Act: offensive, defensive, training, logistics, consequence management

Note that these represent operational functions and not network roles, which are more like military unit support functions, even though some overlap exists. This model can be used to better understand counter-insurgency network requirements and communication flows and to help with friendly force protection needs – especially as parts of the network constantly move through the loop. This model also has utility for targeting non-state opposing forces.

More efficient OODA loop functioning can also be tied into the netwar concept's five levels of analysis. The more evolved a network is in each of these areas the better it is expected to perform:[10]

Organizational: learn to mix hierarchical and network forms in interagency mechanisms
Doctrinal: institute doctrines, operating concepts that match network organization
Technological: develop information, communication systems to serve interagency work
Social: train teams to think and behave in network terms
Narrative: effective 'fight for civilization' based on universal liberal values

These levels of analysis thus have a direct bearing on network issues and dynamics. In addition the primary challenge for counter-insurgency networks (counternetwar) is 'How to make the network a source of loyalty?'[11] Practical observation suggests that loyalty to the network begins to develop when an individual accepts that the network offers new mission capabilities against non-state threats. This acceptance can be derived from a convincing presentation, testimonials, independent research, a gut feeling or an immediate perceived need. That loyalty intensifies after that individual directly experiences network operational utility – during an exercise or an actual incident (operation).

Loyalty to the network can create tension with loyalty to one's hierarchy because different perspectives on cooperation exist. Networks operate as 'non-zero sum games' (everyone benefits) while hierarchies operate as 'zero-sum games' (winners and losers). As a result network nodes will share resources for the common good while stand alone nodes will hoard them for individual gain. Actual network sharing of physical resources has been observed in operational situations.

THE 'TEW' MODEL

One early effort to forge a networked response to post-modern networked threats is found in the terrorism early warning (TEW) group model. The terrorism early warning (TEW) group model was first established in Los Angeles County in 1996 to address the challenges of postmodern terrorism. The TEW follows a networked approach, integrating law enforcement, fire, health and emergency management agencies to address the intelligence needs for terrorism and critical infrastructure protection. The TEW model is based on the premise that intelligence is more than 'secret information' about an adversary. Intelligence to address contemporary threats must go beyond mere descriptions of the threat actors (opposing force, OPFOR); it must also provide a range of users (investigators, emergency responders, planners, etc.) with assessed and accurate information about the situation they are managing.

The TEW model describes this process as 'all source/all phase' fusion. For the TEW, intelligence is derived from all potential sources (classified, sensitive but unclassified, and open sources or OSINT) to provide information at all phases of a threat/response (pre-, trans- and post-incident). The TEW assumes that information germane to an event is available from local through global sources. The immediate precursor for an attack may be in the local area, across the nation, a foreign nation, in cyberspace, or in a combination of all. To achieve this local through global fusion, the TEW relies on a process known as intelligence preparation for operations (IPO).[12] IPO fuses a number of traditional intelligence processes with its own TEW process (which includes evaluating trends and potentials, capabilities and intentions, and providing an operational net assessment depending upon the current position of a threat on a notional event horizon). In short, IPO blends weather, enemy and terrain (WET), with urban IPB (intelligence preparation of the battlefield) and a variety of geospatial and geosocial tools to provide context for anticipating and understanding a suite of potential and actual threats.

The Los Angeles TEW was designed to provide the operational intelligence development of potential courses of action necessary to quickly move through the decision cycle (OODA loop), forecast the potential event horizon, and craft meaningful courses of action for interagency, interdisciplinary response. It relies upon not only the analysis of criminal leads and sensitive sources, but also open source intelligence (OSINT) for scanning/monitoring trends and potentials that provide context for on-going assessment and to influence training and doctrinal needs. Additionally, during an actual threat period or attack, the TEW provides consequence projection (forecasting) to identify potential courses of action to the unified command structure. Essentially, the TEW is an 'all source/all phase' operations-intelligence fusion cell that fuses not only information, but a range of operational entities and intelligence disciplines to develop actionable intelligence products for achieving situational understanding.

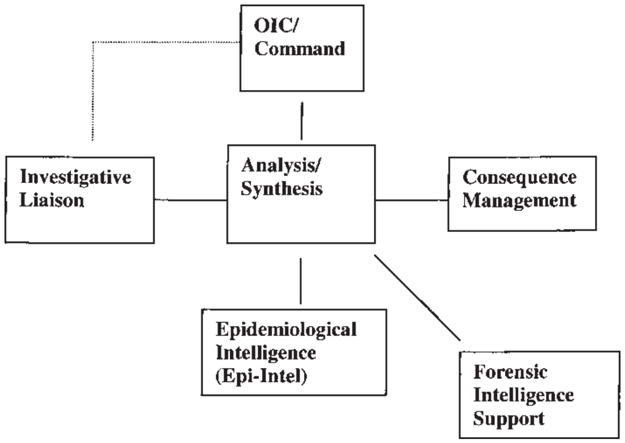
TEW ORGANIZATION

While seeking indications and warning or during an actual event, the TEW utilizes a 'net assessment' process to determine the scope of an actual or potential event and its impact on its area of operations (operational area). Organizationally, the TEW is organized into six cells: the officer-in-charge or OIC (command), analysis/synthesis, consequence management, investigative liaison, epidemiological intelligence (epi-intel) and forensic intelligence support cells. The forensic intelligence support cell, which includes technical means and such external resources as virtual reachback, supports the others (the TEW organization is depicted in Figure 1).

The OIC (command) cell is a team that provides direction, sets intelligence requirements and is responsible for interacting with prevention and response organizations and incident command entities. The analysis/synthesis cell coordinates net assessment activities and develops the collection plan (including tasking requests for information to the various net assessment elements). The analysis/synthesis cell is also responsible for the intake of leads and reports, and developing the results of all the cells' analysis into actionable intelligence products (including advisories, alerts, warnings, and mission folders to assist response).[13] The consequence management cell assesses the law, fire and health (EMS–hospital–operational medical) consequences of the event. The investigative liaison cell coordinates with criminal investigative entities and the traditional intelligence community. the epidemiological intelligence (epi-intel) cell is responsible for real-time disease surveillance and coordination with the disease investigation. Finally, the forensic intelligence support cell exploits a range of technical means to support the TEW fusion process. These include CBRNE reconnaissance,

FIGURE 1

TEW NET ASSESSMENT ORGANIZATION



the use of sensors and detectors, geospatial tools (including mapping, imagery and GIS products), and cyber means.

The TEW model is currently expanding to other jurisdictions. At the time of this writing, there are TEWs at various levels of evolution in Orange, San Bernardino/Riverside, San Diego and Sacramento counties in California. Others also exist in Pierce County (Tacoma), Washington; Tulsa, Oklahoma; Hennepin County (Minneapolis), Minnesota; the National Capital Region (DC, VA, MD), and New Orleans, Louisiana in addition to the initial Los Angeles (LA TEW) group.

These groups are evolving into a network, sharing common organization and doctrine, in order to share threat information and support each other during critical periods. Additionally, the Memorial Institute for the Prevention of Terrorism (Oklahoma City) and the US Department of Homeland Security (Office of Domestic Preparedness) are sponsoring efforts to expand the TEW model into approximately 51 Urban Area Security Initiative (UASI) cities throughout the United States by focusing grant support for TEW initiatives.

NETWORK ISSUES AND DYNAMICS

Counter-terrorism and counter-insurgency networks are a less mature organizational form than law enforcement and military based hierarchies. As a result they are less understood and institutionalized than traditional governmental structures. In fact, from an organizational life cycle perspective these networks represent entrepreneurial (experimental) entities. Their form and functioning is still being ‘worked out’ and many of the potentials they offer are not fully understood.

As can be expected then counter-terrorism/counter-insurgency networks, such as the TEW, face unique challenges. It is expected that over time these challenges will be overcome and they will evolve into institutionalized structures based on common operating procedures and well defined doctrine. In the interim, various issues and dynamics currently exist:

Organizational and Bureaucratic Competition

Networked forms compete with their hierarchical predecessors. Bureaucratic inertia slows moves toward node-to-node and peer-to-peer collaboration both within and especially across disciplines (and jurisdictions). This is complicated by fiscal competition and struggles for intergovernmental primacy. While intelligence fusion groups, like the TEW, seek to serve information requirements of a number of entities to achieve a common operational advantage, some of these entities prefer concentrating (hoarding) information to bolster their organizational position.

Which Entity is in Control?

Within a networked structure, the question of which entity exerts control is unavoidable. This is as true within a single node as within a network of collaborative nodes. During exchanges between different agency personnel one of the first questions is always ‘Who is in control of this group?’ While this is a valid question for hierarchical [line and blocked] based structures it is an inappropriate question concerning networks.[14] Network participation is all about influence – a sharing of ideas and common visions – not control. Depending on the network organization the level of entity influence will shift. All channel networks tend to have nodes with more equal levels of influence than the star structure with more nodal influence concentrated at the hub.

Nodes which refuse to share information and ideas within a network – because of bureaucratic and cultural inhibitions – quickly get labeled as ‘black holes’. These nodes suck up information and ideas but do not contribute to the common good of the network. This fosters distrust within the network. Over time those nodes lose influence within the network and risk being severely limited in their access to network information or, in extreme cases, even dropped from the network. The lack of rigid hierarchy does not mean there is no functional leadership over work processes and information assessment and sharing. Within one node, such as an individual TEW, team leaders and the OIC cell ensure coordination and interaction among cells, as well as with external entities (such as the local, state and federal agencies contributing personnel). As such, an individual TEW is a hybrid organization bridging traditional government hierarchies and network forms.

The organizational dynamics of a network (both within a networked node and among nodes) are influenced by several factors. These include measures of network connectivity and, most importantly, communications. For example, when Valdis Krebs in his paper ‘Uncloaking Terrorist Networks’ described Al Qaeda’s 9/11 network, he identified three metrics: degrees (activity), closeness (access to other nodes), and betweeness (control over information flow).[15] In that analysis Mohammed Atta was identified as a key leader (broker of relationships and information) and the ‘Hamburg cell’ as a key node or hub based upon the denseness of connections within the network.[16] These central positions allow for the most important aspect of network influence: communication. Communication is essential to ensure rapid processing of information and adherence to the network’s narrative vision. Communication is also essential to mitigate the tendencies toward fragmentation that occur as individual nodes become isolated and focused inward or toward other objectives.

Protocols and Rules

Defining and codifying the relations between networked actors is essential to exploiting the benefits of intelligence fusion. Information sharing to counter the evolving terrorist threat can not rely solely on top-down structures. Much of the information necessary to understand the dynamics of the threat, indeed even recognize that there is a threat, is developed from the bottom-up, as well as through multilateral exchanges of information, including indicators of potential attacks and alliances among networked criminal actors. New policy and intergovernmental instruments are needed to fully exploit lateral information-sharing and the development of distributed intelligence processing across organizational and political seams. This includes the development of mechanisms for sharing information among both intra-national and international nodes.

Specialization and Generalization

There is a tension between specialization and generalization. The TEW model fills a specialty niche, assessing and fusing interdisciplinary intelligence for counter-terrorism. Some observers prefer a model that fuses traditional intelligence for a narrower set of users (i.e., the traditional criminal and military services). These are able to focus only on criminal and military threats respectively. In reality, both types of fusion are necessary in a crime–war operational environment. Criminal and military intelligence for a range of threats including criminal enterprises of all sorts (drug cartels, gangs, organized crime, etc.) and terrorism (insurgency) need to be closely aligned with (and exploited by) the specialist TEW model for counter-terrorism intelligence fusion.

Network Scale and Degrees of Separation

Limitations exist concerning how large a network can develop because of information overload and issues of trust. Humans can only filter through so much information before they are overwhelmed. These can be seen on a daily basis concerning e-mails. E-mails serve as a means to an end but can become an end in themselves. Wading each day through thousands of e-mails generated by a network can paralyze all other activities. Intelligence and information collection, exploitation, assessment and visualization tools, such as 'intelligence bots' and other automated tools can help to lessen, but do not fully mitigate, this problem.

In regards to trust, individuals can only maintain so many relationships before they are overwhelmed with relationship maintenance. Relationship maintenance based on phone calls, e-mails and physical meetings will at some point take away from other forms of productivity. While some governmental bureaucrats are able to make a career out of attending meetings, this is the antithesis of counter-insurgency networks. The other aspect of this problem is degrees of separation influencing trust. If a network has too many degrees of separation between the various nodes, trust dissolves. If this happens the network will then begin to break apart. If ignored, hierarchical relationships can once again develop between the dropped nodal linkages and those parts of the network will be lost.

Interface with Hierarchies

Networks can interface with hierarchies in varying ways. They can develop linkages at all levels – strategic, operational and tactical – with the officer-in-charge or OIC (command) link the most prevalent for intelligence support. Tactical links are common for ground sensor and criminal intelligence needs while strategic links may be created for special facility and event access for intelligence preparation for operations.

One of the most problematic interface issues is operational tempo (OPTEMPO). Networks have far quicker reaction cycles than hierarchies because of 'their efficiency and effectiveness in procuring information'[17] This increased OPTEMPO results in the network quickly getting ahead of the hierarchy during an operation or mission. This mismatch in OPTEMPO can create communication problems because the network will be addressing problems that the hierarchy has not yet even identified. These are real life concerns that have been viewed in both exercises and actual operations. Another problem is the fact that a hierarchical based entity may refuse to work with a network. The network is viewed as too alien and/or threatening for the hierarchy's leadership and bureaucracy to interface with. As a result the fear of looking bad can become a concern of more importance for a hierarchy than mission performance.

Public–Private Network Issues

Protecting the postmodern market-state is a complex endeavor. The relationships among the variety of state and non-state actors involved are continually evolving in organizational and legal terms. Much of the critical infrastructure of modern society is privately held and operated. Private corporations and nongovernmental organizations (NGOs) provide telecommunications, information technology, energy, finance, transportation and a range of services traditionally provided by governments. (These corporate entities and NGOs are increasingly trans- and multinational in scope and nature.) The complex interdependencies among these infrastructural sectors and their relationships to governmental organizations are little understood and require a high degree of coordination among operators with sometimes divergent and sometimes convergent interests.

A counter-terrorism or counter-insurgency network will have to interoperate with a number of governmental organizations and entities at the local, state, and federal levels (for example within the US or Canada) or with a number of international or supranational entities (as in the case of the member states of the European Union). In addition, these security networks will have to interact with a number of NGOs, corporate security entities and private military and intelligence providers. Take the case of contemporary crisis and conflict management. A number of humanitarian NGOs, advocacy groups, international organizations (such as the United Nations and its various arms), military and intelligence services of multiple nation-states, and a growing number of private military companies (PMCs) operate to assess, anticipate and respond to crisis. All these diverse and diffuse entities play varying roles in understanding and containing crises and war. Peacemaking, peacekeeping, stability and support operations rely on a complex networked interaction among actors to operate. NGOs such as the International Committee of the Red Cross (ICRC), International Crisis Group, Human Rights Watch, etc. rely upon the services and co-operation of nation-states and their military organs, private security and intelligence contractors, to provide services and build global civil society. The state security services (military and police) also increasingly rely upon private contractors (PMCs and corporate intelligence services) to perform their tasks. Both mechanisms to ensure information-sharing when appropriate and safeguard information and liberties are required, The body of international law, both international criminal law and international humanitarian law (IHL) or the laws of armed conflict have not caught up to these operational realties.

MULTILATERAL COUNTER-INSURGENCY NETWORKS

Understanding and combating contemporary terrorist and insurgent networks requires diverse intelligence and security agencies to pool and aggregate their most precious resource: information. Sharing information and knowledge, and working together to develop useful information or actionable intelligence in the first place requires the development of new networked and distributed security and intelligence structures.

The networked Islamist *jihadi* networks pioneered by Osama bin Laden's Al Qaeda are increasingly being recognized as a global insurgency. These groups, or actually networks of networks, view their war as a global *intifada*. In the aftermath of the Madrid bombings, European police observed that Islamic terrorists evade detection by regrouping and recombining within the framework of loosely organized networks to evade capture and sustain operations. Yet, while the need for closer coordination and cooperation among international police and intelligence services is broadly recognized, barriers to such action are created by divergent judicial and policing systems with investigative cooperation dependent upon an informal 'sneaker net' of magistrates, prosecutors, police and intelligence officers. This is equally true in military as well as civil aspects of counter-terrorism and counter-insurgency. In Iraq insurgents are exploiting networks to recruit fighters, obtain weapons and move funds. These networks exploit criminal enterprises and linkages within the *jihadi* international to seek support from Europe, Asia and elsewhere to prosecute their local insurgency. Such cooperation is forthcoming since *jihadi*s see the Iraqi theatre as only one segment of their global operational space (opspace).

While the *jihadi* international, with Al Qaeda at the vanguard, link many other networks (including notably Jemaah Islamiya and Lasker-e-Toiba) together in their quest for a new caliphate, intelligence services in traditional nation-states face several structural limitations. They are strategically limited in their ability to recognize the extent of the challenge and operationally and tactically challenged in efforts to identify, track and disrupt terrorist networks. Intelligence forums focus on sharing general threat information on regional or transnational issues, but all too often keep specific intelligence to themselves. Obviously, there is a tension between information sharing and operational security to protect sources, means, and interests. Yet, erring too much on the side of secrecy inhibits the ability to quickly and comprehensively identify and counter networked adversaries.

The networks – actually 'multi-networks' or networks of networks – challenging the nation-state are diffuse and exploit secrecy to pursue their global goals. Sometimes they appear acephalous (headless), at others they appear polycephalous (multi-headed). Frequently they employ 'swarming', a tactic where dispersed forces converge or 'swarm' to concentrate, focus, or mass their resources or effort to conduct an attack or campaign. As John Arquilla and David Ronfeldt well observed, 'it takes networks to fight networks'.[18]

The TEW model and its emerging network as described above and elsewhere[19] is an early attempt to develop a counternetwar structure to combat terrorism and insurgency. As Arquilla and Ronfeldt observed, counternetwar relies upon a blurring of offense and defense.[20] This feature is embraced by the TEW model that views prevention and response as points on the continuum of conflict, rather than separate, distinct undertakings. Combating a global insurgency requires an integrated approach. Both prevention and response are influenced by local and global factors, with local and global information requirements at various phases of operations. Such a configuration allows each TEW node to perform dynamic assessment, cutting across 'stovepipes' to configure an adaptive assessment organization that incorporates the internal (intra-node) and external (across nodes) elements necessary to identify specific threats, trends, and potentials. Configuring each node – and ultimately the entire network – to have permeable boundaries that expand capability when needed and exploit distributed subject matter expertise (exploiting the skills and capabilities of other nodes and clusters) to solve a specific problem, allows the network to become agile and adaptive. This allows each node to wield operational capability individually and across the network. Speed, adaptation, and resilience are the anticipated result.

The resulting counter-insurgency network thus will require more than linking disparate databases. It requires building and understanding relationships (individual and organizational) on a multi-lateral basis. As the web 'blog' site 'Global Guerillas' observes,[21] distributed networks have a dynamic, 'non-hierarchical' design, and are actually composed of a 'meta-matrix' of networks for a number of functions: information exchange, knowledge sharing, task completion, etc. As such, they learn and adapt at the individual node and network levels. Many networks are 'scale-free' in configuration. That is, a few nodes have a high degree of connectivity (meaning they become hubs) while others operate with a lesser degree of connectivity. These dynamics are important to consider when developing a counter-terrorism/counter-insurgency network. While individual hubs are important, and hubs with high capacity (early adapters, nodes with high throughput/bandwith, critical skills, etc.) are critical, the workload must be distributed across the network to optimize resilience. Multiple hubs, reinforced by clusters of nodes with distributed capabilities, can absorb both random failure and intentional attack. This is true both for criminal and terrorist networks and networks supporting civil society.

Networks confer many organizational advantages over hierarchies. Closing the gap conferred by these advantages requires the development of counter-terrorist/counter-insurgency networks. A dynamic and decentralized network that avoids over-centralization (a typical bureaucratic reaction to change and its challenges) ensures multilateral information exchange over one-way (usually bottom-up or top-down) information flow through bureaucratic 'stovepipes' is essential. Such a network needs to include nodes at the local level (micro-networks in themselves that integrate all necessary local actors and link with other nodes), a national network, and a broader global network of networks. Such a scalable structure must incorporate real-time information flow and distributed processing, and exploit multiple information sources and types. In such a network, all nodes are users and producers of intelligence. Information and trends from multiple nodes are assembled at individual nodes and collaboratively through node-to-node and peer-to-peer efforts. Information, analysis and intelligence are then shared across all pertinent nodes, exploiting an open architecture. Tailored and ad hoc assessment and project teams can be stood up and demobilized as the situation warrants. Speed, relevance and a common understanding of OPFOR dynamics, organization and evolution can then be assembled and disseminated to those with a need to know.

FUTURE POTENTIALS

The United States individually and the community of nations governed by the rule of law are facing a significant epochal threat. Forging an appropriate response to this evolving threat envelope is a complex and demanding task, demanding significant deliberation in order to develop a balanced approach. Yet this deliberation must occur quickly as the conflict is already in progress and promises to widen. Serious attention must be given to a revision of the entire US national security structure (as well as that of Great Britain, France, the European Union and other international structures) to break down the bureaucratic obstacles to action. Entrenched bureaucratic obstacles are in a true sense real-time barriers to effective efforts to combat terrorism and, if left untended, promise to serve as a force multiplier to the opposing force.

The global war on terrorism is the decisive conflict of the twenty-first century. Global *jihadi* networks are waging a concerted and protracted global insurgency to dominate the post-modern geopolitical landscape. This *intifada* or insurgency comes as the nation-state is negotiating an epochal shift in the organization of the state. Competing views of sovereignty are vying for prominence in the new market-state order. This 'state transition' will no longer tolerate the traditional nation-state view that crime is the purview of single states. Addressing the multinational mercenary terrorist networks of the present and of the future requires new security structures. Philip Bobbitt[22] observes that Osama bin Laden's Al Qaeda is a malignant and mutated version of the market-state. As such, Al Qaeda and its kin are more than stateless gangs. These new networked adversaries possess standing armies, treasury and revenue sources (even if derived from criminal enterprises), a bureaucracy or ‘civil’ service, intelligence collection and analysis organs, welfare systems, and the ability to make alliances (with state and non-state entities). They also promulgate law and policy, and declare war. As such, the Al Qaeda network and others like it are virtual states. These virtual states are non-territorial market-states (although they sometimes hold and control territory) and through insurgency seek to hold or influence more.

Dark or malevolent networks are only one side of the equation. Technology and its impact on social organization are making networks an element of civil society as well. Transnational networks are starting to emerge to counter these threats. The interdependence of contemporary society increasingly relies upon ‘networked civil society’ to address interdependent issues such as transnational organized crime, terrorism, human rights, environment, finance and trade. As such, the globalization of justice and security is in its early stages.[23] Mechanisms to understand and counter the cross-cutting threats of global insurgency, terrorism, and fourth generation warfare to states, regions and economic actors are starting to be formed. A global counter-terrorism and counter-insurgency network (or networks) are necessary to preserve both national and global security during this tumultuous phase.

ACKNOWLEDGEMENTS

This work is partially derived from John P. Sullivan, ‘Networked All-Source Fusion for Intelligence and Law Enforcement Counter-terrorism Response’, paper presented to ‘Integrating Intelligence and Law Enforcement for Homeland Security’, Intelligence Studies Section of the International Studies Association (ISA), 2004 ISA Annual Convention, Montreal, Quebec, Canada, 18 March 2004. Specific observations on the operational capacity and practices of existing counter-terrorism and insurgency efforts and nascent networks are withheld for operational security (OPSEC) purposes.

NOTES

1. Fourth generation warfare (4GW) describes an operational environment where a variety of non-state actors go beyond terrorism (which is a tactic) to challenge the nation-state. See for example, G.I. Wilson, John P. Sullivan and Hal Kempfer, ‘Fourth Generation Warfare: It’s Here, And We Need New Intelligence-gathering Techniques for Dealing with It’, *Armed Forces Journal International*, October 2002, pp.56–62.
2. One early analysis of the potential convergence of narcotics enterprises, terrorists and other networked actors was discussed in Robert J. Bunker and John P. Sullivan, ‘Cartel Evolution: Potentials and Consequences’, *Transnational Organized Crime*, Vol.4, No.2, Summer 1998, pp.55–74.
3. See Robert J. Bunker, *Five-Dimensional (Cyber) Warfighting: Can the Army After Next be Defeated Through Complex Concepts and Technologies?* (Carlisle, PA: US Army War College, Strategic Studies Institute, 1998) for a cogent discussion of the complexities of the evolving threat environment.
4. John Arquilla and David Ronfeldt, ‘The Advent of Netwar (Revisited)’, in John Arquilla and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), pp.7–8.

5. The category of ‘crossovers’ was deleted. ‘Insulators’ were retained but their utility is questionable. Phil Williams, ‘Transnational Criminal Networks’, in John Arquilla and David Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Santa Monica, CA: RAND, 2001), pp.82–4.
6. Richard Rothberg, ‘From the Whole Cloth: Making up the terrorist network’, *Connections*, Vol.24, No.3 (2002), pp.36–42.
7. Vladis E. Krebs, ‘Mapping Networks of Terrorist Cells’, *Connections*, Vol.24, No.3 (2002), pp.31–4.
8. Resources exist on the US military side. FBE Delta noted decrees in decision making, mission timeline, shooter effectiveness, assets scrambled and leaders. *Fleet Battle Experiment Delta Quick Look Report, An Assessment of IT-21 Warfigting Value-Added, 1 Mar 99*.
9. See John R. Boyd, *The Essence of Winning and Losing*, 28 June 1995, available at ⟨http://www.au.af.mil/au.awc⟩ and John R. Boyd, Lecture, US Naval Institute Seminar, Washington, DC, September 1996.
10. John Arquilla and David Ronfeldt, *The Advent of Netwar* (Santa Monica, CA: RAND, 1996), p.33 and the narrative level of analysis in Table 1 of Arquilla and Ronfeldt’s essay in this volume.
11. Arquilla and Ronfeldt, *The Advent of Netwar*, p.33.
12. See Matt Begert and Dan Lindsay, ‘Intelligence Preparation for Operations’, in Robert J. Bunker (ed.), *Non-State Threats and Future Wars* (London: Frank Cass, 2003), pp.133–43.
13. Mission Folders are incident-specific tools to assist incident commanders; they include real-time threat information and estimates, technical information and potential courses of action.
14. See Table 1 concerning the differences between these organizational forms, in Barry Wellman, ‘The Rise (and Possible Fall) of Networked Individualism’, *Connections*, Vol.24, No.3 (2002), pp.30–32.
15. Valdis E. Krebs, ‘Uncloaking Terrorist Networks’, FirstMonday, Vol.7, No.4, (April 2002), available at ⟨www.firstmonday.dk/issues/issue7_4/krebs⟩.
16. Ibid.
17. Phil Williams, ‘The Nature of Drug-Trafficking Networks’, *Current History* Vol.97, No.618 (April 1998), p.156.
18. Arquilla and Ronfeldt, ‘The Advent of Netwar (Revisited)’, p.15.
19. For additional information on the prospects for the TEW model to serve as a counternetwar structure see John P. Sullivan, ‘Networked Force Structure and C^4I’, in Robert J. Bunker (ed.), *Non-State Threats and Future Wars* (London: Frank Cass, 2003), pp.144–58.
20. Arquilla and Ronfeldt, ‘The Advent of Netwar (Revisited)’, p.12.
21. ‘Global Guerrillas’ is one of the many emerging web ‘blog’ sites seeking to understand and navigate the changing, networked dynamics of post-modern conflict. The site carries the kicker ‘The next generation of terrorism. How it will develop and how it will be fought.’ See ⟨http://globalguerillas.typepad.com⟩.
22. Philip Bobbitt (like others) argues that an epochal shift in the organization of states is underway. Bobbitt posits that the new state form supplanting the nation-state is the market-state. Within that analysis, he sees terrorist networks (with Al Qaeda being an early example) as a malevolent form of market-state. See Philip Bobbitt, *The Shield of Achilles: War, Peace, and the Course of History* (New York: Anchor Books, 2002), esp. pp.820–21.
23. See Anne-Marie Slaughter, *A New World Order* (Princeton, NJ: Princeton University Press, 2004).